国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 11 月 18 日-2024 年 11 月 24 日 **2024 年第 47 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 325 个，其中高危漏洞 160 个、中危漏洞 149 个、低危漏洞 16 个。漏洞平均分值为 6.65。本周收录的漏洞中，涉及 0day 漏洞 239 个（占 74%），其中互联网上出现“Tenda AC 10U 堆栈缓冲区溢出漏洞（CNVD-2024-45806）、OneBlog 跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的漏洞总数 3062 个，与上周（19639 个）环比减少 84%。

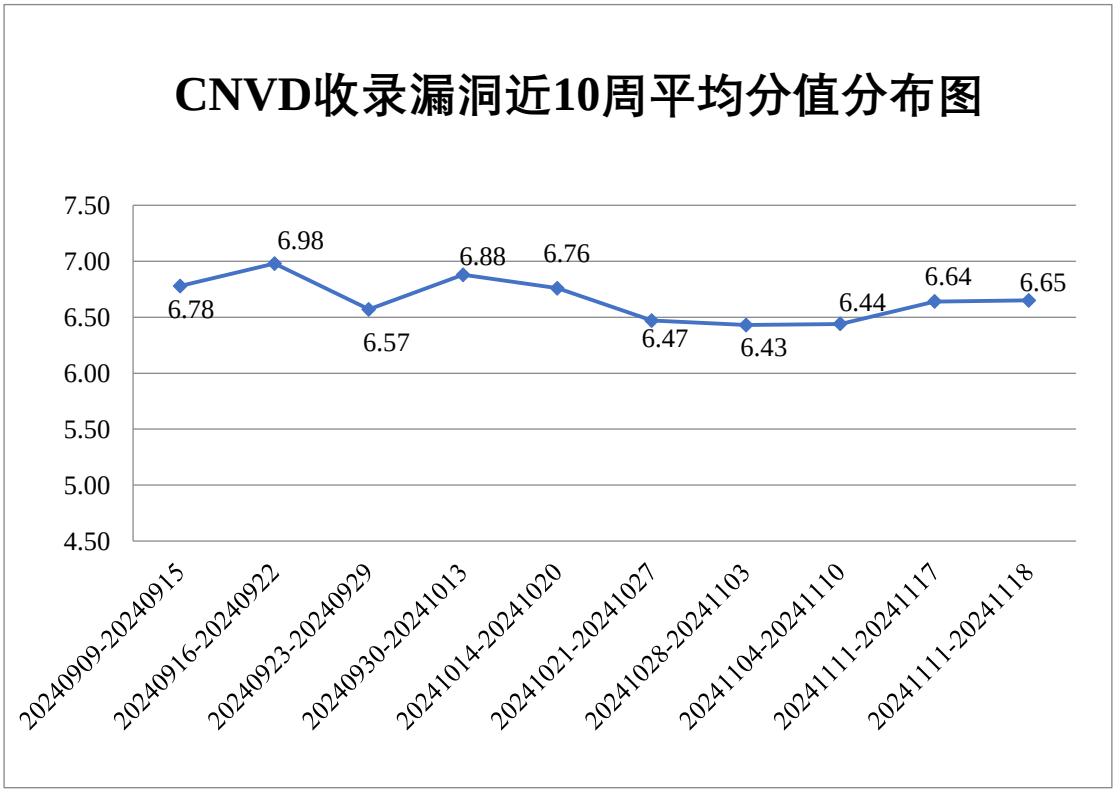

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 4 起，向基础电信企业通报漏洞事件 2 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 762 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 68 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 16 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

中电科金仓（北京）科技股份有限公司、瑞斯康达科技发展股份有限公司、广东保伦电子股份有限公司、北京北大方正电子有限公司、用友网络科技股份有限公司、理光（中国）投资有限公司、上海曼恒数字技术股份有限公司、柯尼卡美能达集团、深圳市乙辰科技股份有限公司、上海冰峰计算机网络技术有限公司、北京星网锐捷网络技术有限公司、厦门四信物联网科技有限公司、深圳市和为顺网络技术有限公司、百度安全应急响应中心、北京惠朗时代科技有限公司、上海海典软件股份有限公司、全讯汇聚网络科技（北京）有限公司、北京华宇信息技术有限公司、畅捷通信息技术股份有限公司、苏州欧信达信息科技有限公司、深圳市蓝凌软件股份有限公司、安徽生命港湾信息技术有限公司、福建四创软件有限公司、北京中创视讯科技有限公司、北京网动网络科技股份有限公司、腾讯安全应急响应中心、北京亿赛通科技发展有限责任公司、上海企望信息科技有限公司、北京金和网络股份有限公司、普联技术有限公司、南京帆软软件有限公司、深圳市吉祥腾达科技有限公司、中科方德软件有限公司、申瓯通信设备有限公司、北京神州视翰科技有限公司、迈普通信技术股份有限公司、深圳达实物联网技术有限公司、深圳市云盟智慧科技有限公司、上海七慧网络科技有限公司、惠州市德赛智储科技有限公司、北京万户网络技术有限公司、吉翁电子（深圳）有限公司、深圳市鸿升光通讯设备有限公司、ONKYO 安桥安桥（上海）商贸有限公司、佐藤自动识别系统国际贸易（上海）有限公司、北京人大金仓信息技术股份有限公司、广州网易计算机系统有限公司、广州市保伦电子有限公司、杭州迪普科技股份有限公司、北京山石网科信息技术有限公司、北京智芯微电子科技有限公司、智互联（深圳）科技有限公司、郑州市金水区恒友摄影软件经营部、深圳市东宝信息技术有限公司东莞分公司、上海金慧软件有限公司、妈妈在线国际网络科技有限公司、北京致远互联软件股份有限公司、蓝卓数字科技有限公司、天津环球磁卡集团有限公司、泛微网络科技股份有限公司、北京龙软科技股份有限公司、杭州恩软信息技术有限公司、上海灵当信息科技有限公司、安徽阳光心健科技发展有限公司、深圳市思迅软件股份有限公司、翰霖科技股份有限公司、深圳迈贝尔科技有限公司、深圳国威电子有限公司、科华数据股份有限公司、安科瑞电气股份有限公司、北京字节跳动科技有限公司、保定乐活网络科技有限公司、阿里巴巴集团安全应急响应中心、青岛东软载波科技股份有限公司、富士胶片商业创新（中国）有限公司、融智通科技（北京）股份有限公司、上海华测导航技术股份有限公司、西安优迈智

慧矿山研究院有限公司、厦门科拓通讯技术股份有限公司、北京统御至诚科技有限公司、湖南众合百易信息技术有限公司、南京博纳睿通软件科技有限公司、杭州海康威视数字技术股份有限公司、北京润乾信息系统技术有限公司、网是科技股份有限公司、北京趋势威尔网络技术有限公司、郑州金鼓通信技术有限公司、苏州汇川技术有限公司、四川掌上时代科技有限公司、江苏麦维智能科技有限公司、四川易泊时捷智能科技有限公司、深圳市众磊鑫物流有限公司、东莞市同享软件科技有限公司、山石网科通信技术（北京）有限公司、中通云仓科技有限公司、索尼（中国）有限公司、杭州码里码外网络科技有限公司、广州市超易信息科技有限公司、重庆中联信息产业有限责任公司、杭州席媒科技有限公司、烽火通信科技股份有限公司、北京中控智慧科技发展有限公司、北京亚控科技发展有限公司、广联达科技股份有限公司、哈尔滨新中新电子股份有限公司、廊坊市极致网络科技有限公司、龙采科技集团有限责任公司、企查查科技股份有限公司、厦门四信通信科技有限公司、深圳齐心好视通云计算有限公司、深圳市中科网威科技有限公司、神州数码控股有限公司、统信软件技术有限公司、信呼、英飞达软件（上海）有限公司和友讯电子设备（上海）有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天津市国瑞数码安全系统股份有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、新华三技术有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。成都卫士通信息安全技术有限公司、河南东方云盾信息技术有限公司、江苏金盾检测技术股份有限公司、淮安易云科技有限公司、北京翰慧投资咨询有限公司、江苏云天网络安全技术有限公司、北京中睿天下信息技术有限公司、北京山石网科信息技术有限公司、贵州多彩网安科技有限公司、湖南泛联新安信息科技有限公司、福建福诺移动通信技术有限公司、江苏君立华域信息安全技术股份有限公司、江苏正信信息安全测试有限公司、联通数字科技有限公司、中孚安全技术有限公司、北京天下信安技术有限公司、上海蜚语信息科技有限公司、江苏耘和计算机系统工程有限公司、江苏保旺达软件技术有限公司、四川汉安数智科技有限公司、北京卓识网安技术股份有限公司、卫士通（广州）信息安全技术有限公司、保定超安网络科技有限公司、成都安美勤信息技术股份有限公司、江苏省公用信息有限公司、北京安华金和科技有限公司、成都久信信息技术股份有限公司、宁夏凯信特信息科技有限公司、江苏韫道信息安全技术有限公司、北京时代新威信息技术有限公司、深圳市博通智能技术有限公司、北京纽盾网安信息技术有限公司、中华人民共和国广东海事局、国网浙江省电力有限公司电力科学研究院、上海吨吨信息技术有限公司、中资网络信息安全科技有限公司、北京比瓴科技有限公司、深圳昂楷科技有限公司、江苏锋刃信息科技有限公司、北京安帝科技有限公司及其他个人白帽子向 CNVD 提交了 3062 个以事件型漏

洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）和三六零数字安全科技集团有限公司、上海交大向 CNVD 共享的白帽子报送的 1774 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
天津市国瑞数码安全系统股份有限公司	3460	0
北京神州绿盟科技有限公司	1339	155
深信服科技股份有限公司	1018	9
斗象科技（漏洞盒子）	885	885
新华三技术有限公司	869	0
三六零数字安全科技集团有限公司	446	446
上海交大	443	443
北京数字观星科技有限公司	433	0
安天科技集团股份有限公司	431	0
阿里云计算有限公司	332	0
南京众智维信息科技有限公司	123	4
北京知道创宇信息技术有限公司	115	2
京东科技信息技术有限公司	112	4
杭州安恒信息技术股份有限公司	103	1
北京启明星辰信息安全技术有限公司	88	16
远江盛邦（北京）网络安全科技股份有限公司	65	65
厦门服云信息科技有限公司	46	0

北京天融信网络安全技术有限公司	19	19
北京长亭科技有限公司	17	7
杭州迪普科技股份有限公司	10	0
华为技术有限公司	9	9
快页信息技术有限公司	8	8
奇安信网神（补天平台）	4	4
北京智游网安科技有限公司	4	4
北京信联数安科技有限公司	1	1
北京安信天行科技有限公司	1	1
成都卫士通信息安全技术有限公司	55	55
河南东方云盾信息技术有限公司	35	35
江苏金盾检测技术股份有限公司	15	15
淮安易云科技有限公司	14	14
北京翰慧投资咨询有限公司	13	13
江苏云天网络安全技术有限公司	13	13
北京中睿天下信息技术有限公司	11	11
西门子（中国）有限公司	10	0
北京山石网科信息技术有限公司	9	9

贵州多彩网安科技有限公司	8	8
湖南泛联新安信息科技有限公司	5	5
福建福诺移动通信技术有限公司	5	5
江苏君立华域信息安全技术股份有限公司	4	4
江苏正信信息安全测试有限公司	3	3
联通数字科技有限公司	3	3
中孚安全技术有限公司	3	3
北京天下信安技术有限公司	2	2
上海蜚语信息科技有限公司	2	2
江苏耘和计算机系统工程有限公司	2	2
江苏保旺达软件技术有限公司	2	2
四川汉安数智科技有限公司	2	2
北京卓识网安技术股份有限公司	2	2
卫士通（广州）信息安全技术有限公司	2	2
保定超安网络科技有限公司	2	2
成都安美勤信息技术股份有限公司	2	2
江苏省公用信息有限公司	1	1
北京安华金和科技有	1	1

限公司		
成都久信信息技术股份有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
江苏韫道信息安全技术有限公司	1	1
北京时代新威信息技术有限公司	1	1
深圳市博通智能技术有限公司	1	1
北京纽盾网安信息技术有限公司	1	1
中华人民共和国广东海事局	1	1
国网浙江省电力有限公司电力科学研究院	1	1
上海吨吨信息技术有限公司	1	1
中资网络信息安全科技有限公司	1	1
北京比瓴科技有限公司	1	1
深圳昂楷科技有限公司	1	1
江苏锋刃信息科技有限公司	1	1
北京安帝科技有限公司	1	1
个人	749	749
报送总计	11370	3062

本周漏洞按类型和厂商统计

本周，CNVD 收录了 325 个漏洞。WEB 应用 175 个，网络设备（交换机、路由器

等网络端设备）74 个，应用程序 46 个，操作系统 14 个，智能设备（物联网终端设备）10 个，安全产品 5 个，数据库 1 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
WEB 应用	175
网络设备（交换机、路由器等网络端设备）	74
应用程序	46
操作系统	14
智能设备（物联网终端设备）	10
安全产品	5
数据库	1

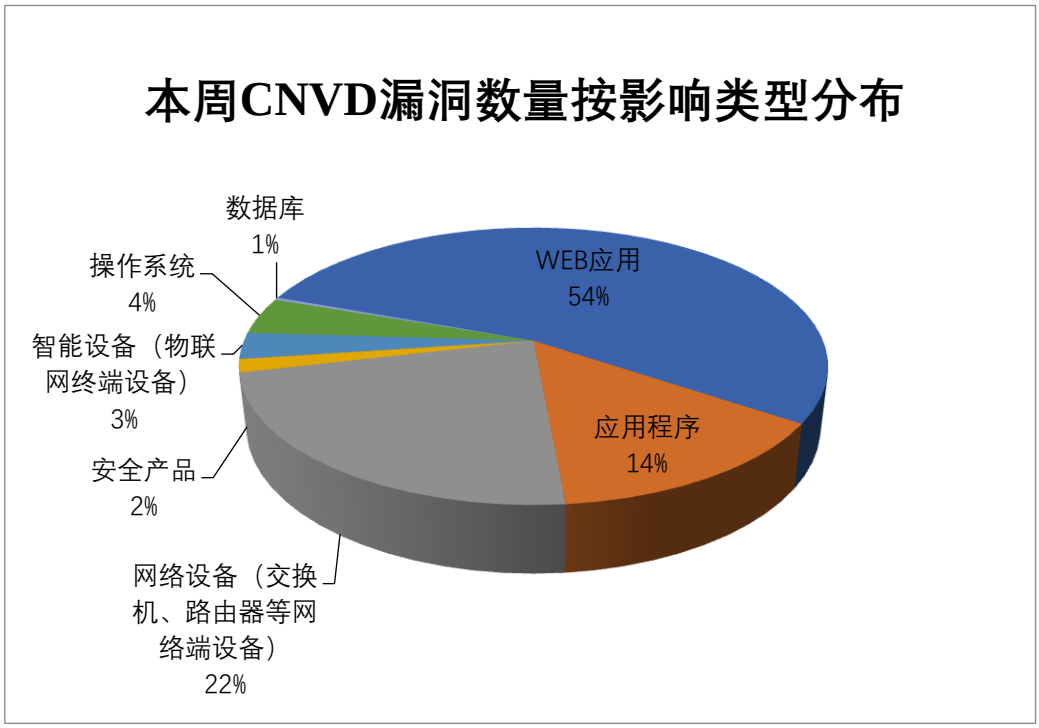

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、用友网络科技股份有限公司、D-Link 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Siemens	19	6%
2	用友网络科技股份有限公司	14	4%
3	D-Link	14	4%
4	Cisco	12	4%
5	Google	11	3%

6	Tenda	10	3%
7	Microsoft	9	3%
8	NETGEAR	8	3%
9	瑞斯康达科技发展股份有限公司	7	2%
10	其他	221	68%

本周行业漏洞收录情况

本周，CNVD 收录了 39 个电信行业漏洞，23 个移动互联网行业漏洞，9 个工控行业漏洞（如下图所示）。其中，“NETGEAR R8500 wiz_fix2.cgi 组件命令注入漏洞、Google Android 权限提升漏洞（CNVD-2024-45229）、多款 Siemens 产品输入验证错误漏洞（CNVD-2024-45210）”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

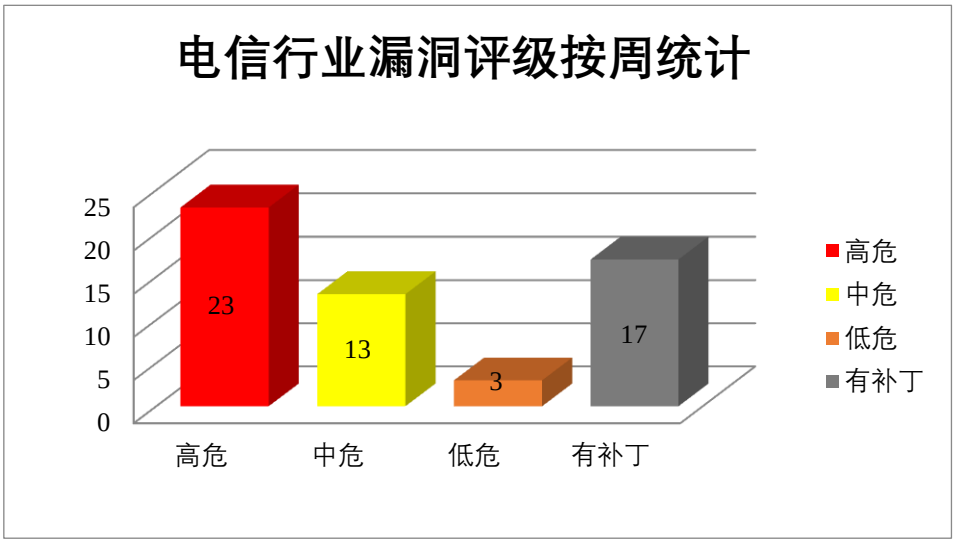

图 3 电信行业漏洞统计

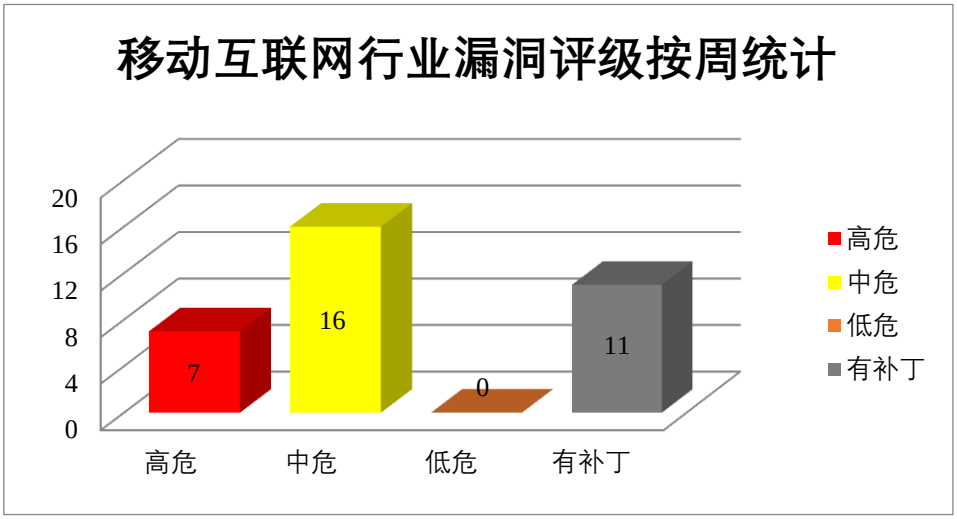

图 4 移动互联网行业漏洞统计

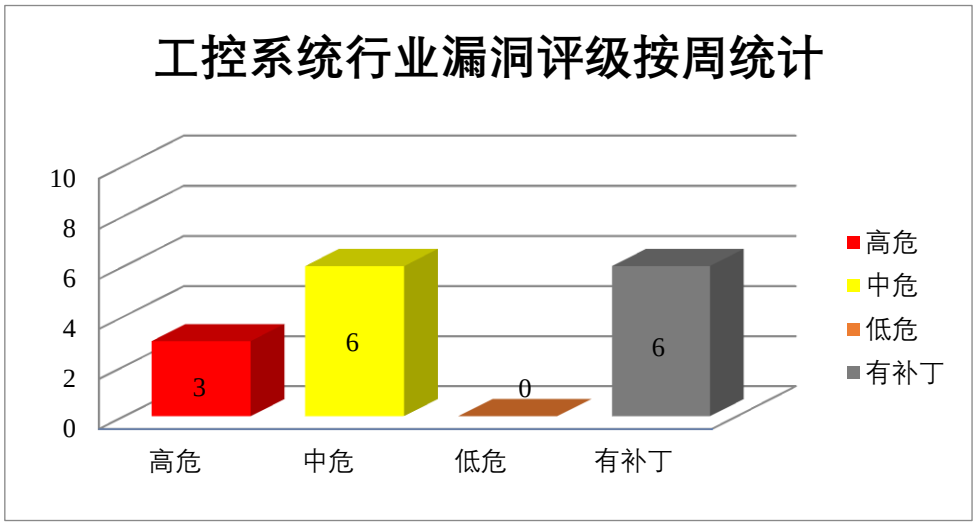

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，升级权限。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2024-45222、CNVD-2024-45229、CNVD-2024-45230、CNVD-2024-45231、CNVD-2024-45232、CNVD-2024-45233、CNVD-2024-45234）、Google Android 信息泄露漏洞（CNVD-2024-45226）。其中，除“Google Android 信息泄露漏洞（CNVD-2024-45226）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-45222
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45226
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45229
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45230
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45231
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45232
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45233
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45234

2、 Microsoft 产品安全漏洞

Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。Microsoft Windows Hyper-V 是微软开发的一种虚拟化技术，主要用于在 Windows 操作系统上创建和管理虚拟机，Shared Virtual Disk 是其中的共享虚拟磁盘。Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。Microsoft LightGBM 是美国微软（Microsoft）公司的一个使用基于树的学习算法的梯度提升框架。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Excel 远程代码执行漏洞（CNVD-2024-45315、CNVD-2024-45317、CNVD-2024-45316、CNVD-2024-45319、CNVD-2024-45318）、Microsoft Windows Hyper-V Shared Virtual Disk 权限提升漏洞、Microsoft Exchange Server 欺骗漏洞（CNVD-2024-45320）、Microsoft LightGBM 远程代码执行漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-45315
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45317
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45316
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45319
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45318
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45321
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45320
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45323

3、 Siemens 产品安全漏洞

Siemens SINEC INS 是德国西门子（Siemens）公司的一款为网络基础设施提供中央服务的软件。SCALANCE M-800，MUM-800 和 S615 以及 RUGGEDCOM RM1224 是工业路由器。SIMATIC S7-PLCSIM 模拟 S7-1200，S7-1500 和其他一些 PLC 衍生产品，作为 SIMATIC STEP 7 的一部分发货。SIMATIC step7（TIA Portal）是一个用于

配置和编程 SIMATIC 控制器的工程软件。simmocode ES 是 simmocode pro 配置、调试、操作和诊断的核心软件包。SINAMICS Startdrive 调试软件是在 TIA Portal 中集成 SINAMICS 驱动器的工程工具。TIA Portal 是一款 PC 软件，可提供从数字规划和集成工程到透明操作的全套西门子数字化自动化服务。TIA Portal Cloud 使得在虚拟化环境中使用 TIA Portal 的主要包和主要选项包成为可能。SINEC NMS 是面向数字化企业的新一代网络管理系统。该系统可以实现对网络的集中监控、管理和配置。Solid Edge 是一个软件工具组合，可解决各种产品开发过程：3D 设计，仿真，制造和设计管理。SIPORT 是一个全面、模块化和可靠的系统，用于监控访问套件中的访问控制和时间管理。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞将任意内容写入主机系统文件中的任何位置，在当前进程的上下文中执行代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens SINEC INS 路径遍历漏洞（CNVD-2024-45208）、Siemens SINEC INS 操作系统命令注入漏洞（CNVD-2024-45206）、多款 Siemens 产品输入验证错误漏洞（CNVD-2024-45210）、多款 Siemens 产品访问控制错误漏洞（CNVD-2024-45209）、多款 Siemens 产品反序列化漏洞、Siemens SINEC NMS 权限分配错误漏洞、Siemens Solid Edge 越界读取漏洞（CNVD-2024-45218）、Siemens SIPORT 权限提升漏洞。其中，“Siemens SINEC INS 路径遍历漏洞（CNVD-2024-45208）、Siemens SINEC INS 操作系统命令注入漏洞（CNVD-2024-45206）、多款 Siemens 产品输入验证错误漏洞（CNVD-2024-45210）、Siemens Solid Edge 越界读取漏洞（CNVD-2024-45218）”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-45208

https://www.cnvd.org.cn/flaw/show/CNVD-2024-45206

https://www.cnvd.org.cn/flaw/show/CNVD-2024-45210

https://www.cnvd.org.cn/flaw/show/CNVD-2024-45209

https://www.cnvd.org.cn/flaw/show/CNVD-2024-45214

https://www.cnvd.org.cn/flaw/show/CNVD-2024-45219

https://www.cnvd.org.cn/flaw/show/CNVD-2024-45218

https://www.cnvd.org.cn/flaw/show/CNVD-2024-45221

4、 Cisco 产品安全漏洞

Cisco Meeting Server（Acano Conferencing Server）是美国思科（Cisco）公司的一套包含音频、视频的会议服务器软件。Cisco Identity Services Engine 是美国思科（Cisco）公司的一款环境感知平台。Cisco Small Business Routers 是一款美国思科（Cisco）公司的一个路由器设备。Cisco Unified Industrial Wireless Software 是思科公司提供的一款用于工业无线网络的软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在受影响的系统上以明文形式查看敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Cisco Meeting Server 信息泄露漏洞（CNVD-2024-45293）、Cisco Identity Services Engine Web 接口跨站脚本漏洞（CNVD-2024-45298、CNVD-2024-45297、CNVD-2024-45296、CNVD-2024-45295）、Cisco Small Business WEB 接口命令注入漏洞、Cisco Small Business WEB 接口远程命令执行漏洞、Cisco Unified Industrial Wireless Software 命令注入漏洞。其中，“Cisco Small Business WEB 接口命令注入漏洞、Cisco Small Business WEB 接口远程命令执行漏洞、Cisco Unified Industrial Wireless Software 命令注入漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-45293
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45298
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45297
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45296
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45295
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45302
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45301
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45300

5、D-Link DSL6740C 操作系统命令注入漏洞（CNVD-2024-45428）

D-Link DSL6740C 是中国友讯（D-Link）公司的一款无线 VDSL 路由器。本周，D-Link DSL6740C 被披露存在操作系统命令注入漏洞，攻击者可利用该漏洞在系统上执行任意命令。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-45428

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2024-45305	NETGEAR R8500 usb_remote_smb_conf.cgi 组件命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.netgear.com/about/security/
CNVD-2024-45215	Siemens TeleControl Server Basic 反序列化漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.industry.siemens.com/cs/ww/en/view/109975921/
CNVD-2024	Microsoft Excel 远程代码执	高	厂商已发布了漏洞修复程序，请及

-45319	行漏洞（CNVD-2024-45319）		时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49026
CNVD-2024-45212	多款 Siemens 产品释放后重用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-354112.html
CNVD-2024-45499	北京亿赛通科技发展有限责任公司电子文档安全管理系统存在 SQL 注入漏洞（CNVD-2024-45499）	高	厂商已提供漏洞修补方案，建议用户下载使用：https://update.nsfocus.com/update/listCdgDetail/v/cdg820-old https://update.nsfocus.com/update/listCdgDetail/v/new-system5.6.2
CNVD-2024-45301	Cisco Small Business WEB 接口远程命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV
CNVD-2024-45307	NETGEAR R8500 wiz_fix2.cgi 组件命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.netgear.com/about/security/
CNVD-2024-45316	Microsoft Excel 远程代码执行漏洞（CNVD-2024-45316）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49027
CNVD-2024-45498	北京亿赛通科技发展有限责任公司电子文档安全管理系统存在 SQL 注入漏洞（CNVD-2024-45498）	高	厂商已提供漏洞修补方案，建议用户下载使用：https://update.nsfocus.com/update/listCdgDetail/v/cdg820-old https://update.nsfocus.com/update/listCdgDetail/v/new-system5.6.2
CNVD-2024-45812	用友网络科技股份有限公司 U8CRM 存在 SQL 注入漏洞（CNVD-2024-45812）	高	厂商已发布补丁修复漏洞，请广大用户及时下载更新：https://security.yonyou.com/#/noticeInfo?id=607

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，升级权限。此外，Microsoft、Siemens、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞将任意内容写入主机系统文件中的任何位置，在受影响的系统上以明文形式查看敏感信息，在当前进程的上下文中执行代码，造成拒绝服务等。另外，D-Link DSL6740C 被披露存在操作系统命令注入漏洞，攻击者可利用该漏洞在系统上执行任意

命令。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、Tenda AC10U 堆栈缓冲区溢出漏洞（CNVD-2024-45806）

验证描述

Tenda AC10U 是中国腾达（Tenda）公司的一款无线路由器。

Tenda AC10U 存在堆栈缓冲区溢出漏洞，该漏洞源于文件/goform/SetPptpServerCfg 的函数 formSetPPTPServer 的参数 endIP 未能正确验证输入数据的长度大小，攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务。

验证信息

POC 链接：https://github.com/abcdefg-png/IoT-vulnerable/blob/main/Tenda/AC10U/v1.V15.03.06.48/more/formSetPPTPServer.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-45806

信息提供者

新华三技术有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. VMware vCenter Server 远程代码执行漏洞正被黑客广泛利用

据 Cyber Security News 消息，博通发布了紧急警告，称 VMware vCenter Server 中的两个关键漏洞现在正被广泛利用。

参考链接：https://www.freebuf.com/news/415580.html

2. 关键的 WordPress 插件漏洞导致超 400 万网站暴露

据 Wordfence 安全研究员披露，一个关键的认证绕过漏洞被暴露在 WordPress 的 Really Simple Security（以前称为 Really Simple SSL）插件中，如果此漏洞被利用，攻击者可以远程获得易受攻击网站的完全管理权限。

参考链接：https://www.freebuf.com/news/415637.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂

商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国计算机网络应急处理体系中的牵头单位。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537